Cybersecurity in the Cherenkov Telescope Array

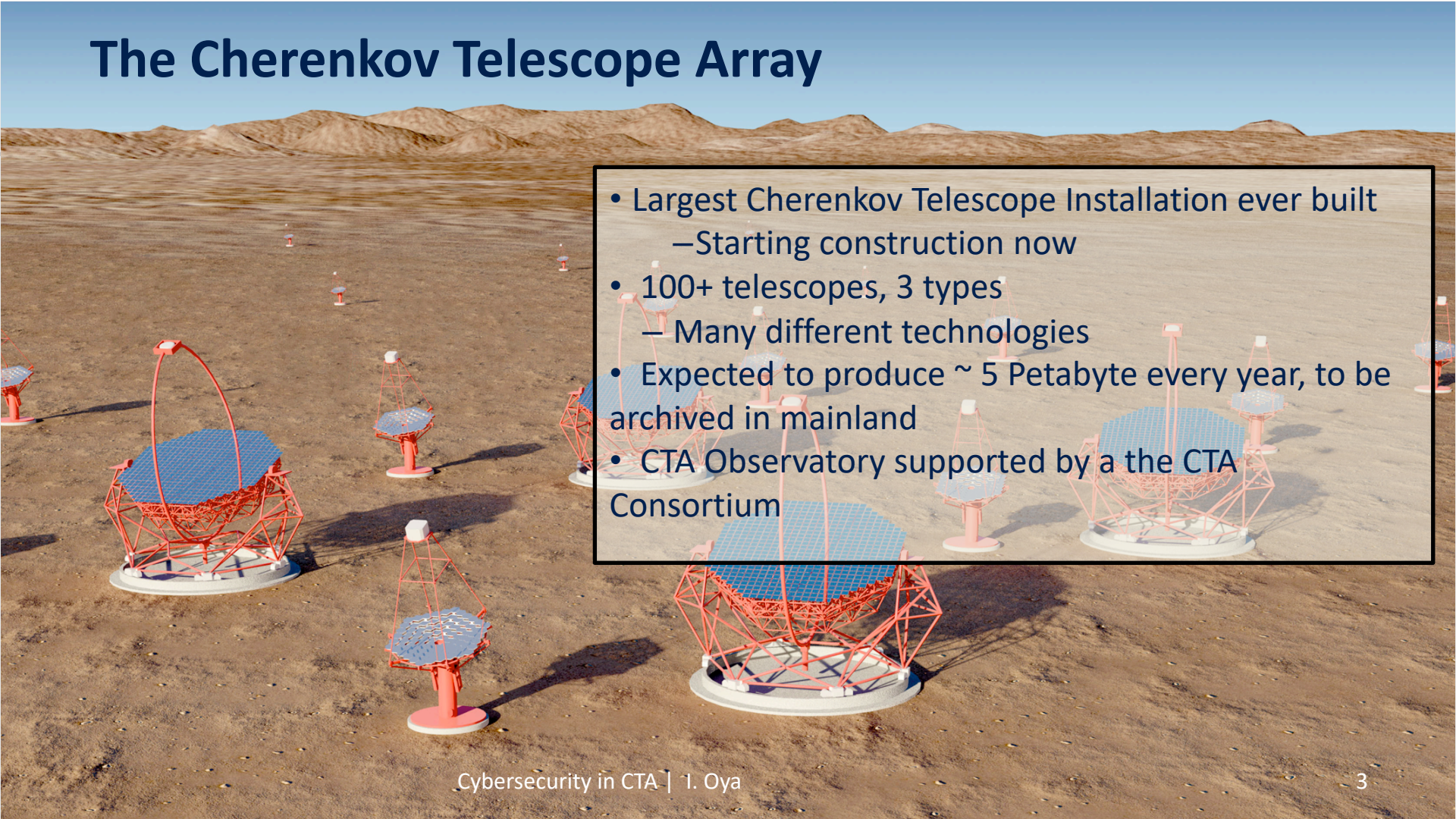
I. Oya
CTA Observatory

Introduction

- Disclaimer:
  - I am a SW team coordinator and not a security expert
  - CTA organization is being set up:
    - No security governance
    - System configuration not fully defined

- Goal: Present CTA project and some of its challenges in terms of security

The Cherenkov Telescope Array

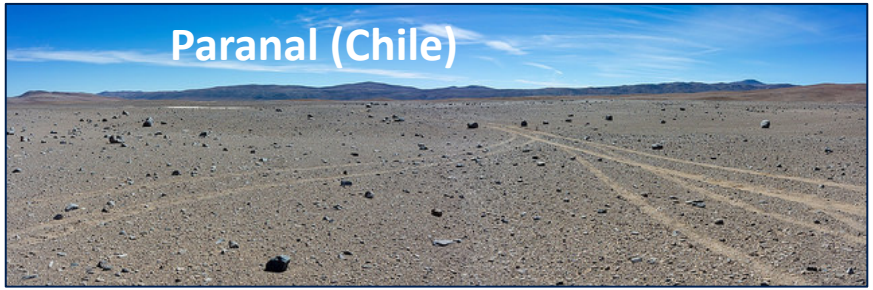


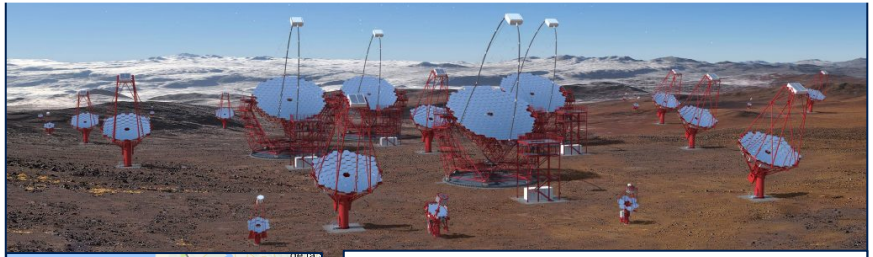
- Largest Cherenkov Telescope Installation ever built
  - –Starting construction now
- 100+ telescopes, 3 types
  - – Many different technologies
- Expected to produce ~ 5 Petabyte every year, to be archived in mainland
- CTA Observatory supported by a the CTA Consortium

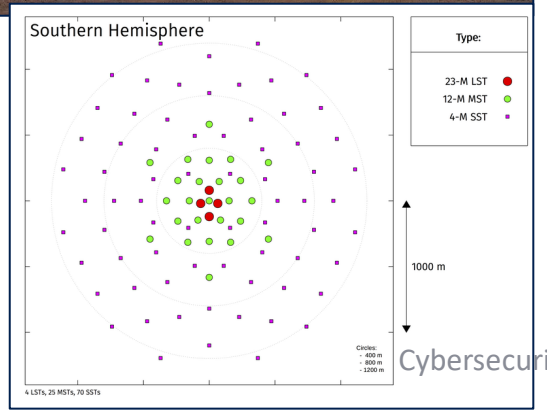
CTA Sites

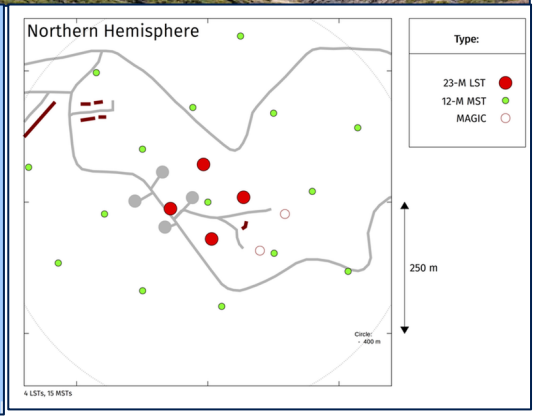

Zeuthen
DESY
Spain
La Palma
Bologna
INAF
northern hemisphere
southern hemisphere
Chile
Paranal
ap: ©2015 Google, Inst. Geogr. Nacional
©2015 Google
Array Sites
Headquarters
Science Management Centre

CTA at Paranal & La Palma







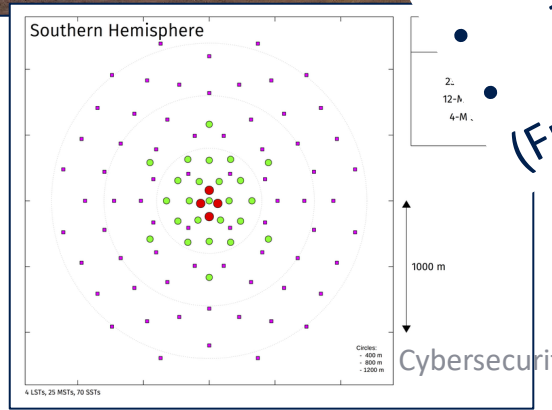


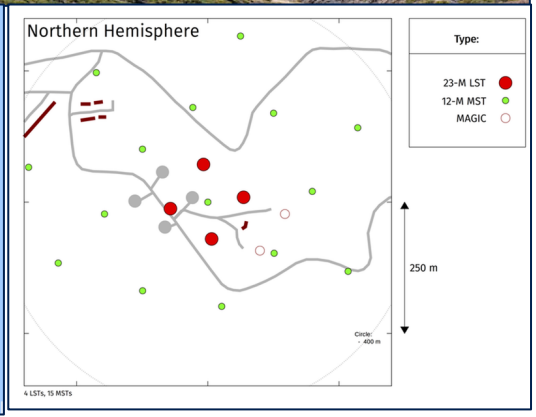
CTA at Paranal & La Palma

Status: no equipment in place

Status:

- 1st telescope being commissioned
- A computer cluster (2k cores, 3 PB) in place
- (Fujitsu, maintenance contract)





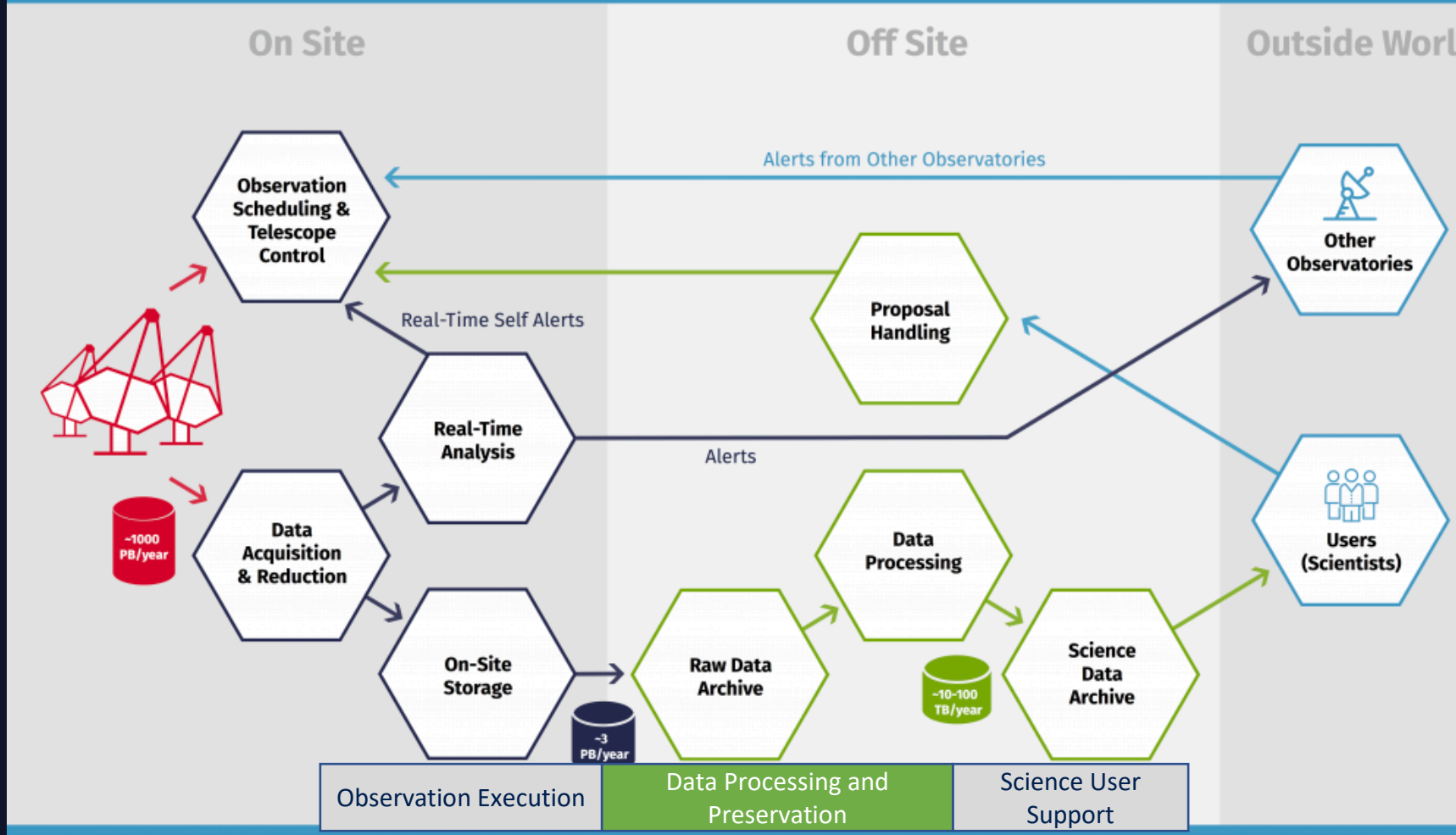
CTAO Legal Entity

- CTA Observatory gGmbH (2014) responsible of CTA implementation:
  - CTAO Staff: 30 persons (Jan 2019) – Expect to arrive to ~80 staff
- The final legal entity for full construction, a *European Research Infrastructure Consortium* (ERIC), is being set up under European Union law (2020?)
- ~70% Construction based on IKCs to the CTA ERIC

The CTA consortium (CTAC)

31 Countries
203 Institutes
1451 Members

CTAO OPERATIONS



Main CTA Systems

Science Operations

- Array Control and Data Acquisition (ACADA)
- Data Processing and Preservation System (DPPS)
- Science User Support System (SUSS)
- Science Operations Support System (SOSS)

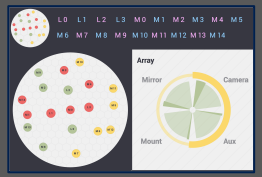
Technical Infrastructure

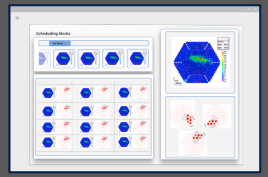
- Telescope (TEL) [*]
- Safety System
- Auxiliary Instruments (AUX)
- Array Infrastructure Elements (AIE)

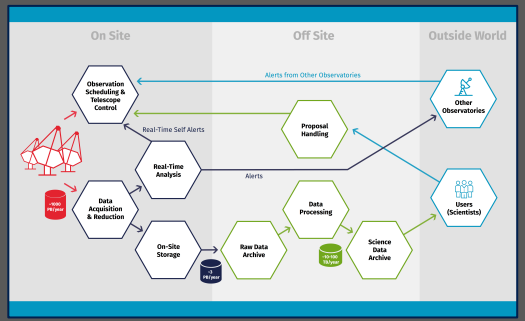
[*] 1 to N telescope systems, several types

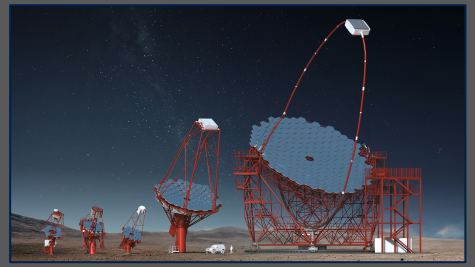
Observatory Operations and Administration

- Technical Operations Support System (TOSS)
- Management and Administrative System (MAS)









Main CTA Systems

Control Systems

Science Operations

SCADA

- Array Control and Data Acquisition (ACADA)
- Data Processing and Preservation System (DPPS)
- Science User Support System (SUSS)
- Science Operations Support System (SOSS)

Technical Infrastructur

Device Control System

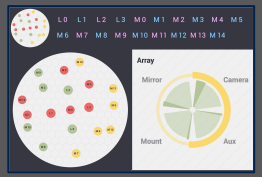
- Telescope (TEL) [*]
- Safety System
- Auxiliary Instruments (AUX)
- Array Infrastructure Elements (AIE)

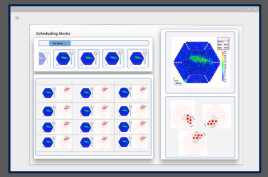
[*] 1 to N telescope systems, several types

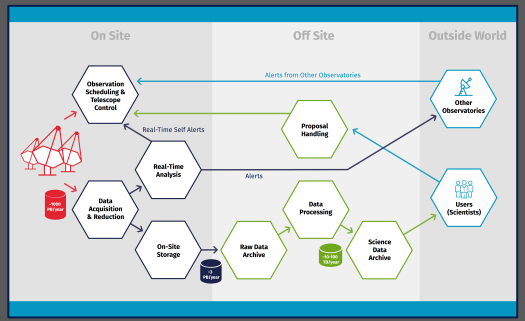
Observa tions and A ion

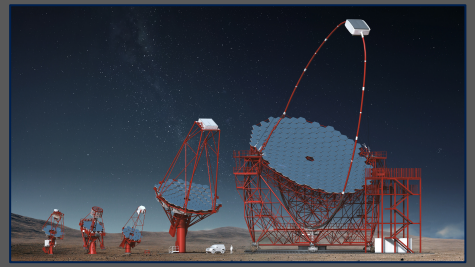
Device Control System

- Technical Operations Support System (TOSS)
- Management and Administrative System (MAS)









CTA Project – Cybersecurity status

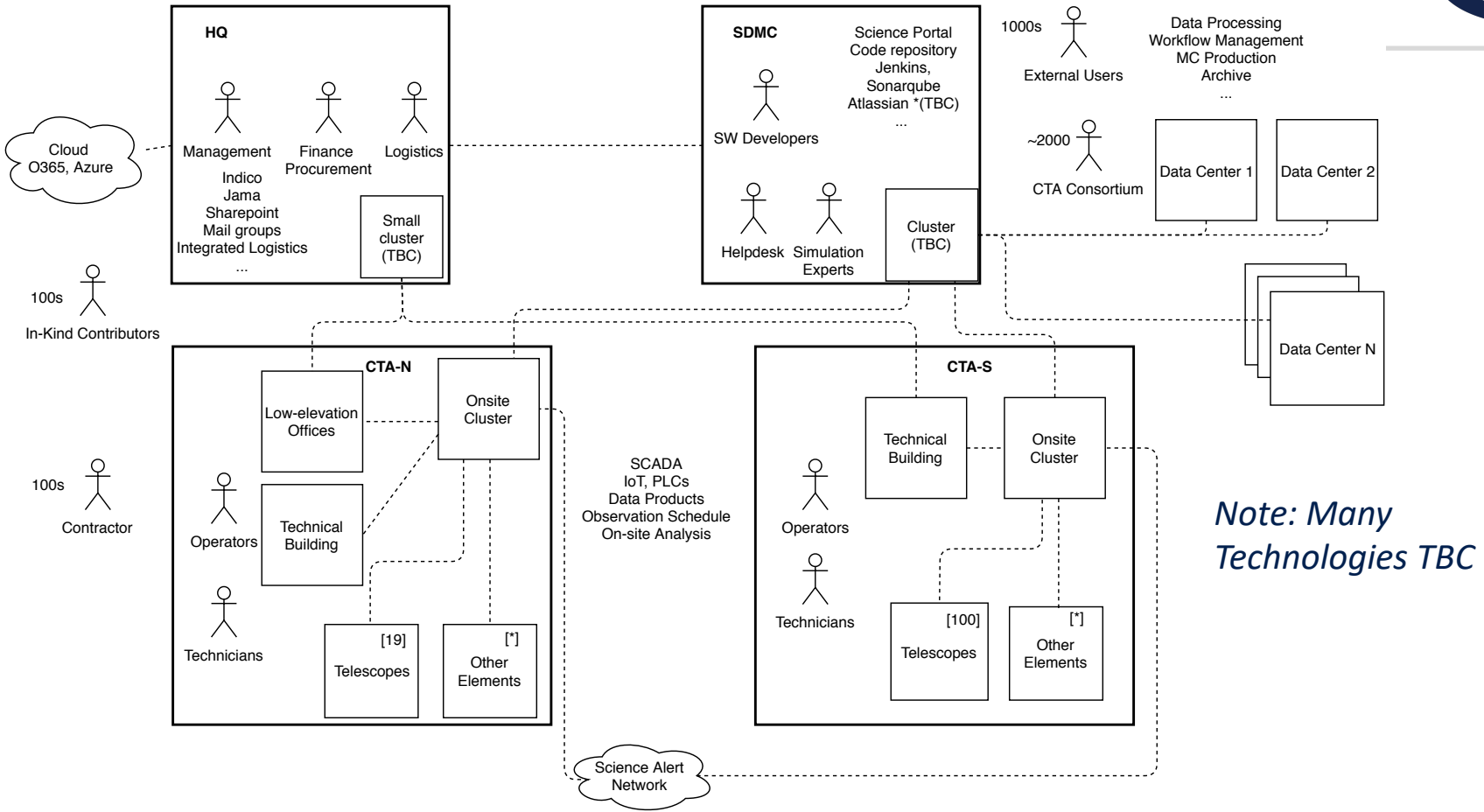
Main Issues

- There is no Cybersecurity concept in the project
- There is no person who feels responsible of cybersecurity at the level of organization
- System configuration & inventory of assets not yet defined

In place:

- Collaborating data centers (in mainland) have each their own well-stablished policies
- CTA-N IT Container delivered by Fujitsu, consultancy by DESY IT experts
- CTA observatory sites (ESO, IAC) with own policies

CTA Elements

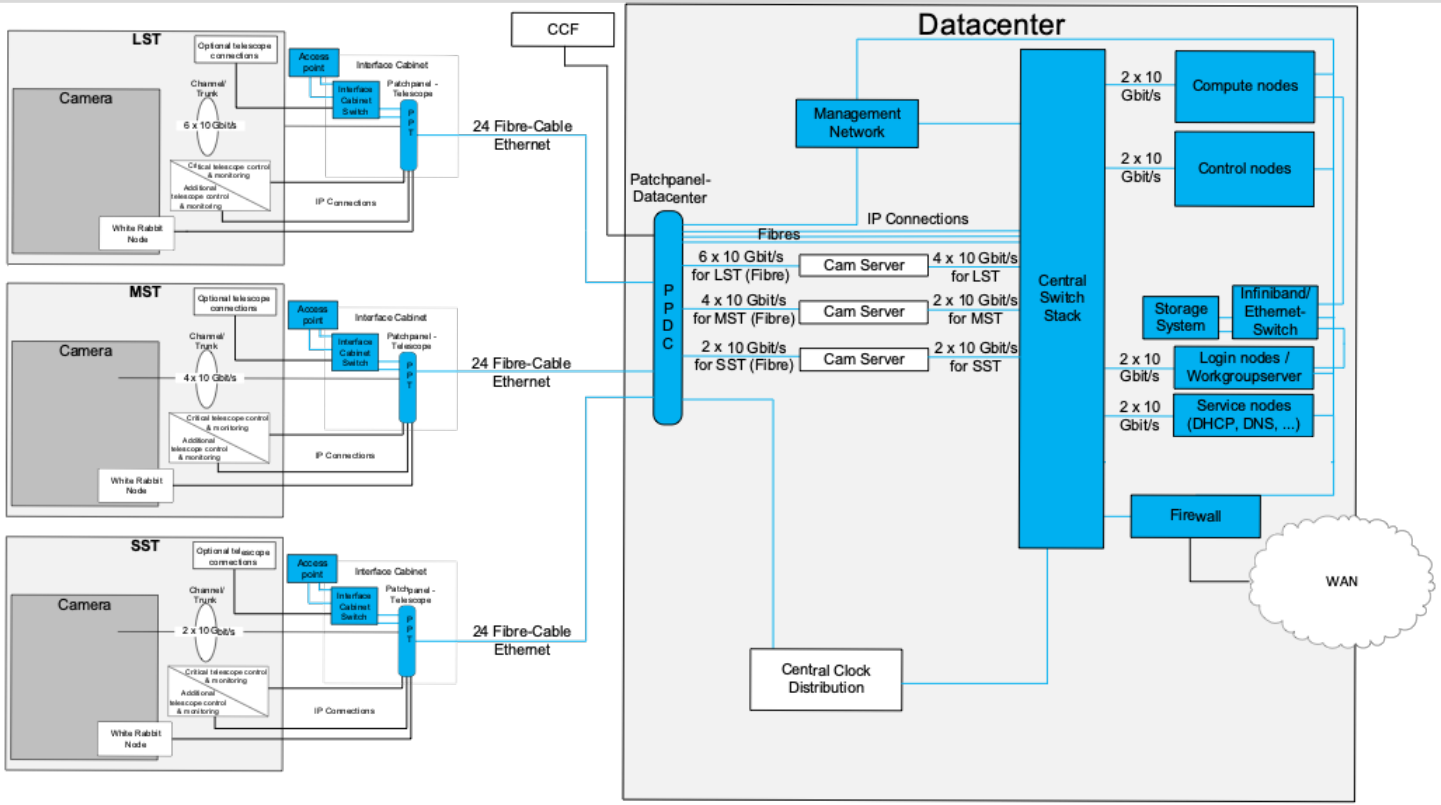


Note: Many Technologies TBC

Control systems- Specific issues

- Vulnerabilities in our control software could create safety risks
  - E.g. point the mirrors to burn the bushes
- Technology choices taken without considering security at all
  - Often chosen by the IKCs “bottom-up”
- Standardization on the way, but not consolidated
  - OPC UA proposed but not fully accepted yet
  - Many runtime environment: various PLCs, NI boxes, RPis, Arduinos, Xbee…., custom
- Inventory of computing equipment or technologies not yet existing
- Remote location – expectations of remote operations incl. control systems
- During constructions: simultaneous deployment of various IKC teams, contractors, staff

Concept & Design for CTA On-Site ICT Infrastructure



Expected technologies on the sites (I)

- Computer cluster with Red Had / CentOS
- Ethernet cable network with fibre, copper and InfiniBand
- Wireless access points around telescopes
- Siemens, Bosch-Rexroth, Beckoff, Panasonic, NI PLCs.
- Embedded machines:
  - Raspberry Pi
  - Arduino
  - NI Boxes
  - Compact desktop machines
  - …
- Onboard Ethernet & wireless devices:
  - CCD Cameras
  - mirror actuators
  - calibration light sources
  - …
- White rabbit for time sync + GPS clocks

Technologies not 100% consolidated

Expected technologies on the sites (II)

- Java, C/C++, Python, JavaScript
- OPC UA (various vendors and embedded in PLC)
- Alma Common Software (CORBA-based framework)
- ZeroMQ
- Low-level: UDP, TCP/IP sockets, raw Ethernet…
- Condition monitoring software boxes with ”whatever-comes-inside”.
- Containers: singularity, docker
- VMs: Virtualbox, Vagrant
- JavaScript-based user interface
- Control rooms at each site
  - One at the site (100s m)
  - At low elevation (~40 km away)

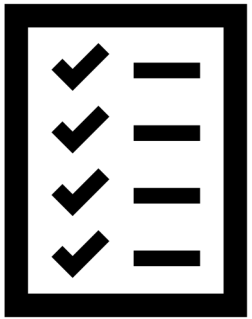
Technologies not 100% consolidated

1st internal workshop on CTA Cybersecurity

- Focused on control systems & on-site
- External consultants from GTD
- Experts from DESY Zeuthen, CTA Personnel, S. Lueders (CERN)
- Went over the project situation, analysed using NIST framework
  - Recommendations by GTD

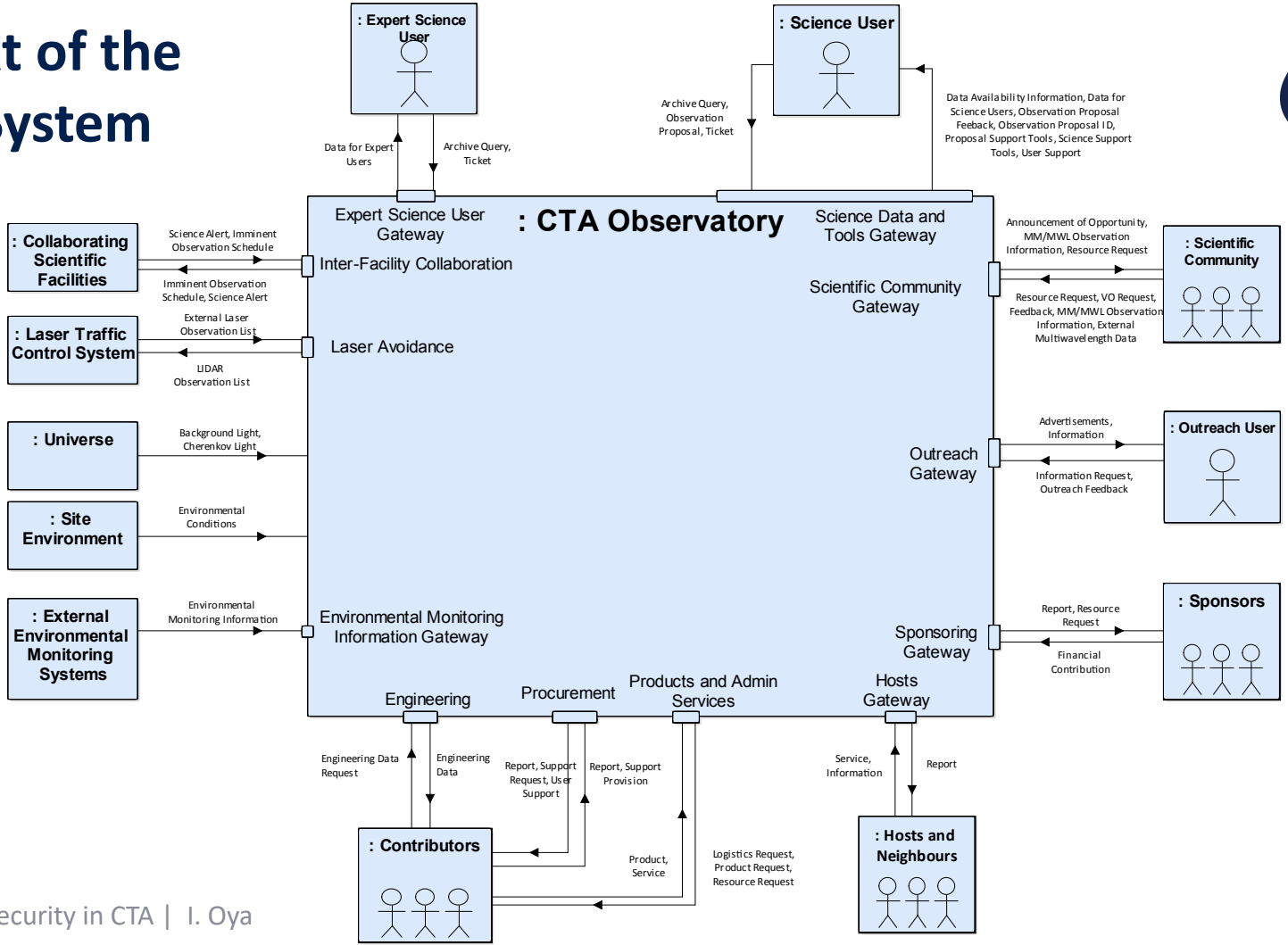
Main action items

- Set-up cybersecurity Governance and roles
  - Planning to announce a CISO position
- Establish associated processes at each location: HQ, SDMC, CTA-N, CTA-S
- Build an asset Inventory. This will help us to organize
  - Consolidate technologies
  - Patch management
  - Malware protection
  - System hardening
- Architecture
  - network segregation and segmentation
- Prepare an A&A system
  - Aim for multi-factor Authentication
- Set up logging and monitoring
- IT/OT Dependency analysis
- Organize vulnerability scans and pentesting
- Awareness training program

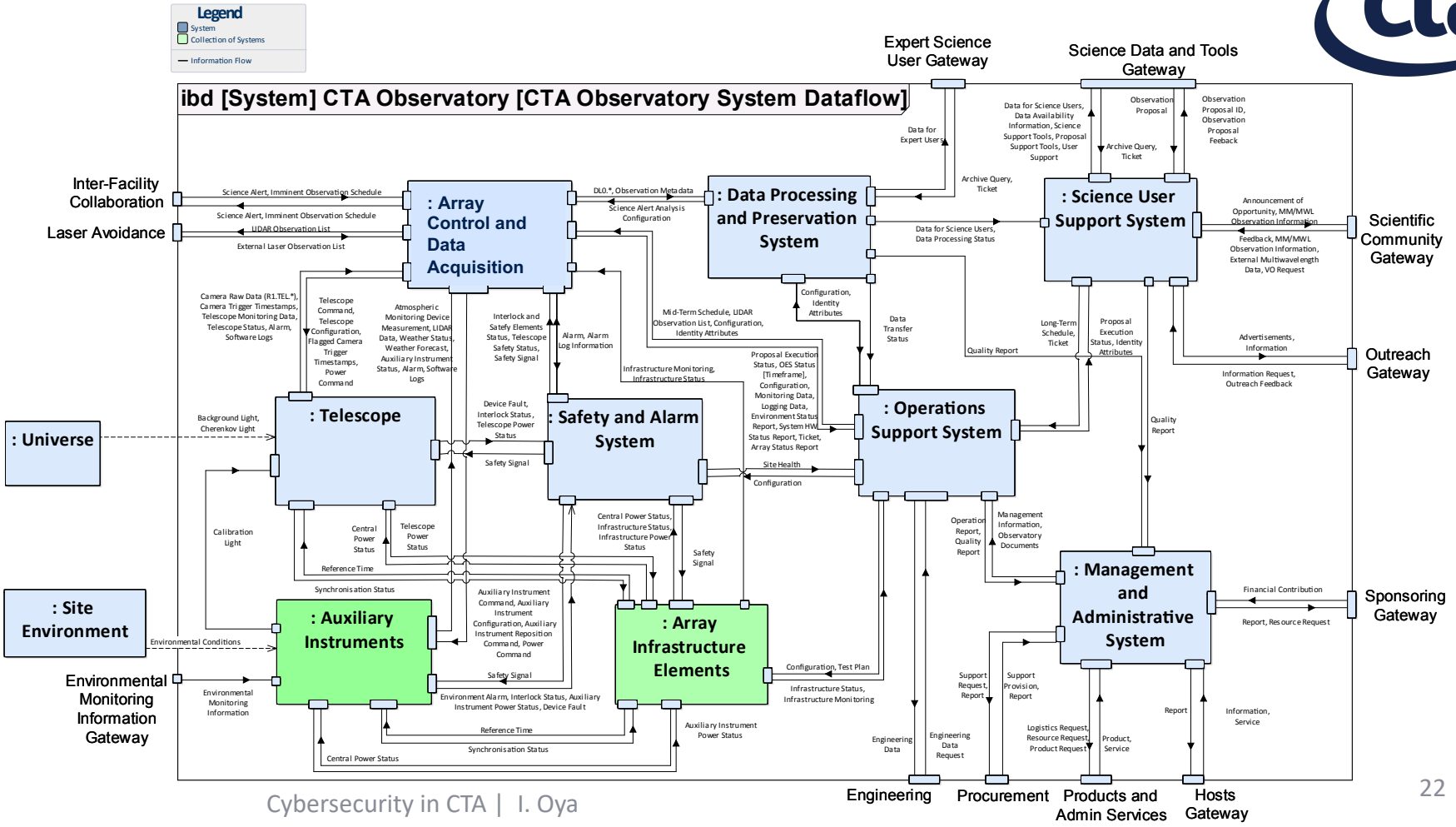


BACKUP

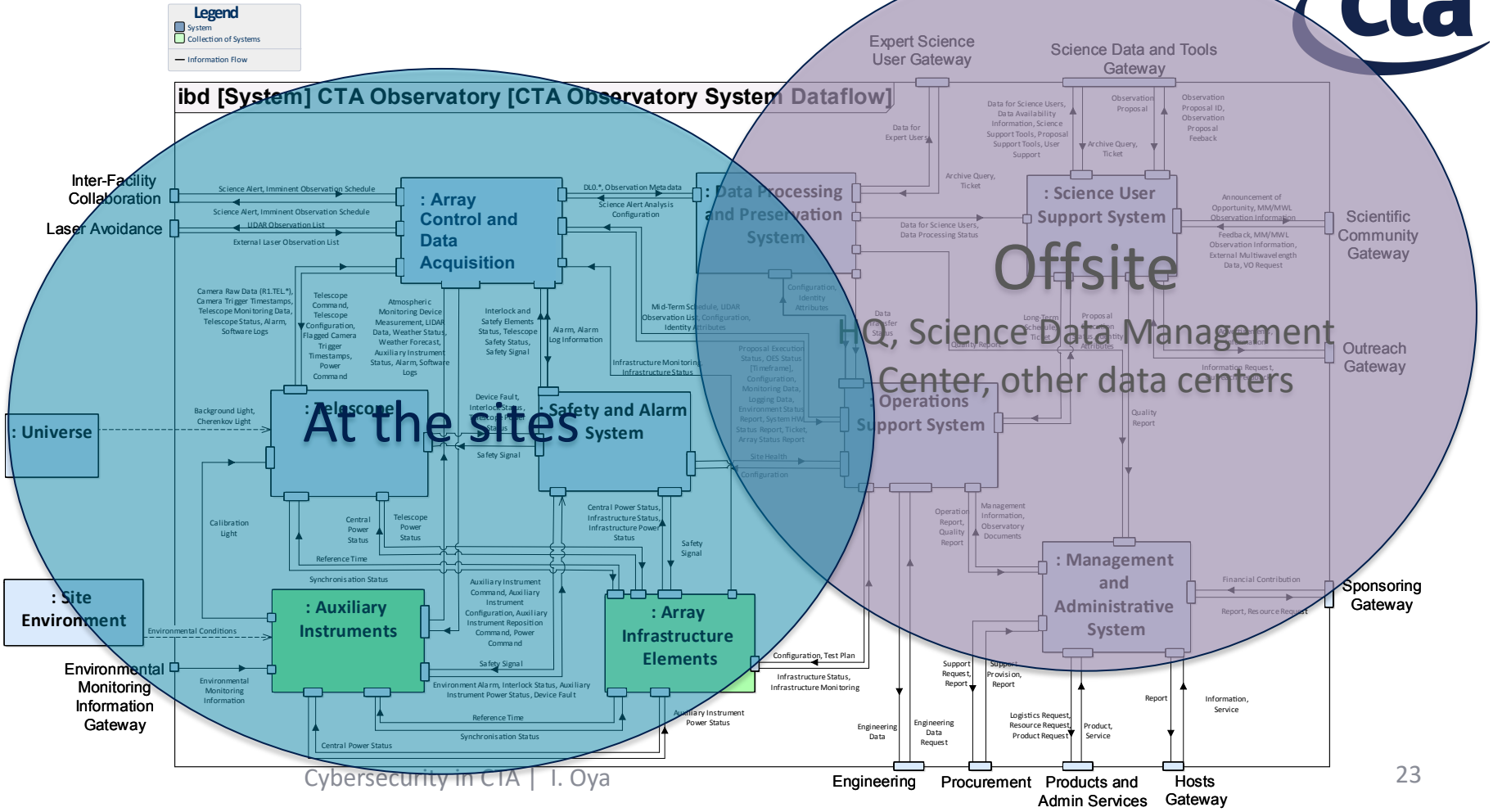
Context of the CTAO System



The CTA System Structure

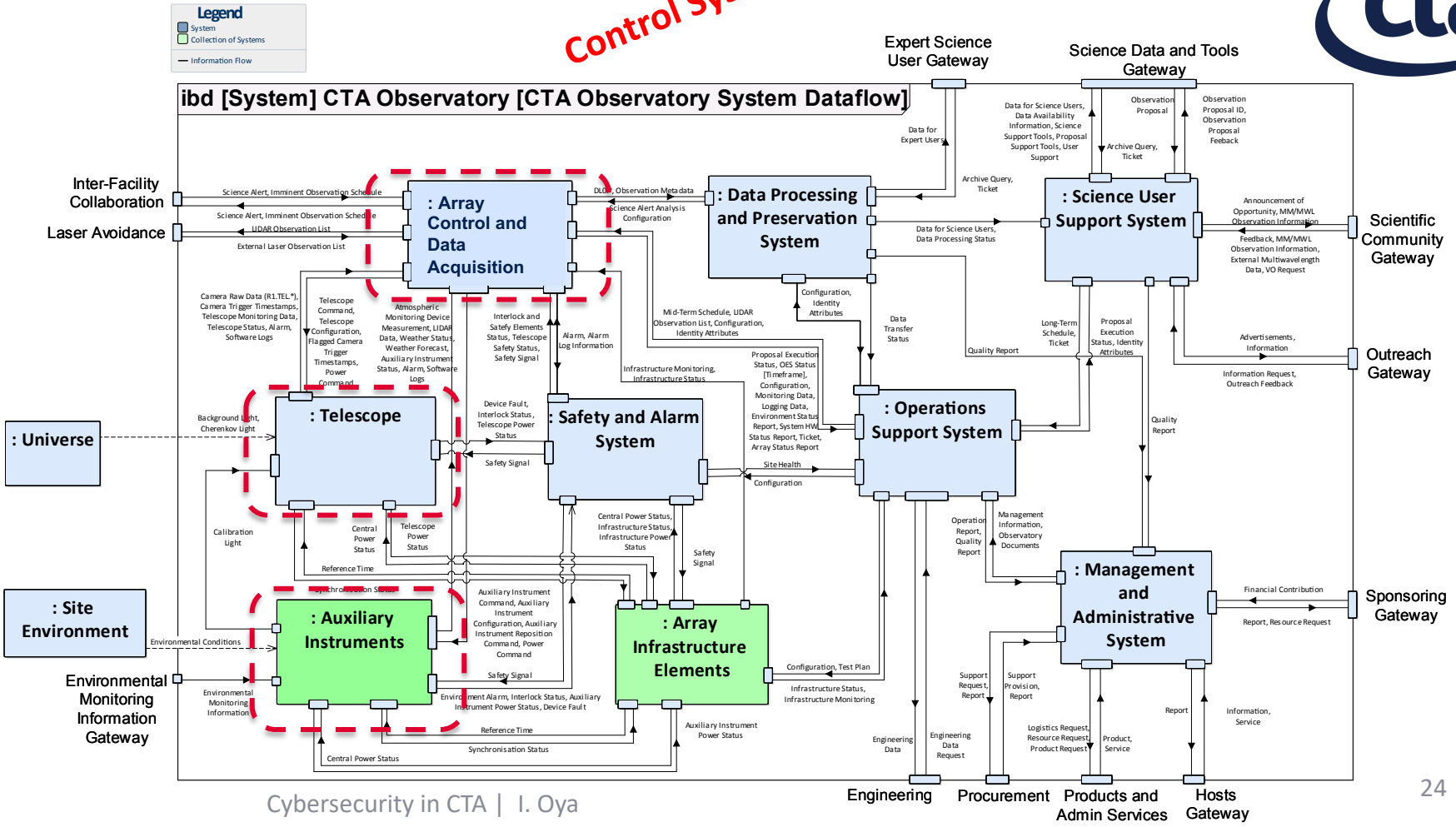


The CTA System Structure

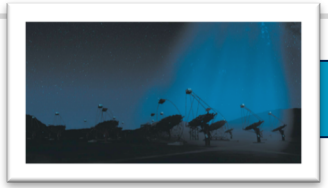


The CTA System Structure

Control Systems



Data Flow – From the Cameras to the User



Array of telescopes

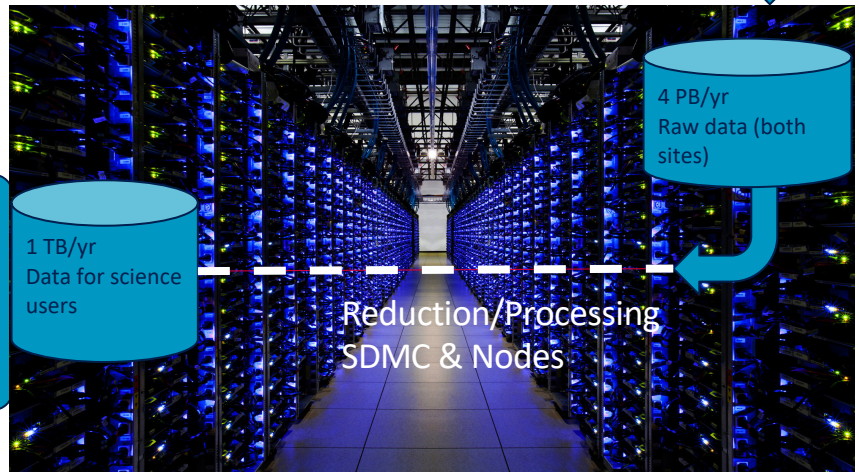
600 Gb/s
(1000 PB/yr)

Reduction at the site

(South site example)

Limited bandwidth

1 Gb/s



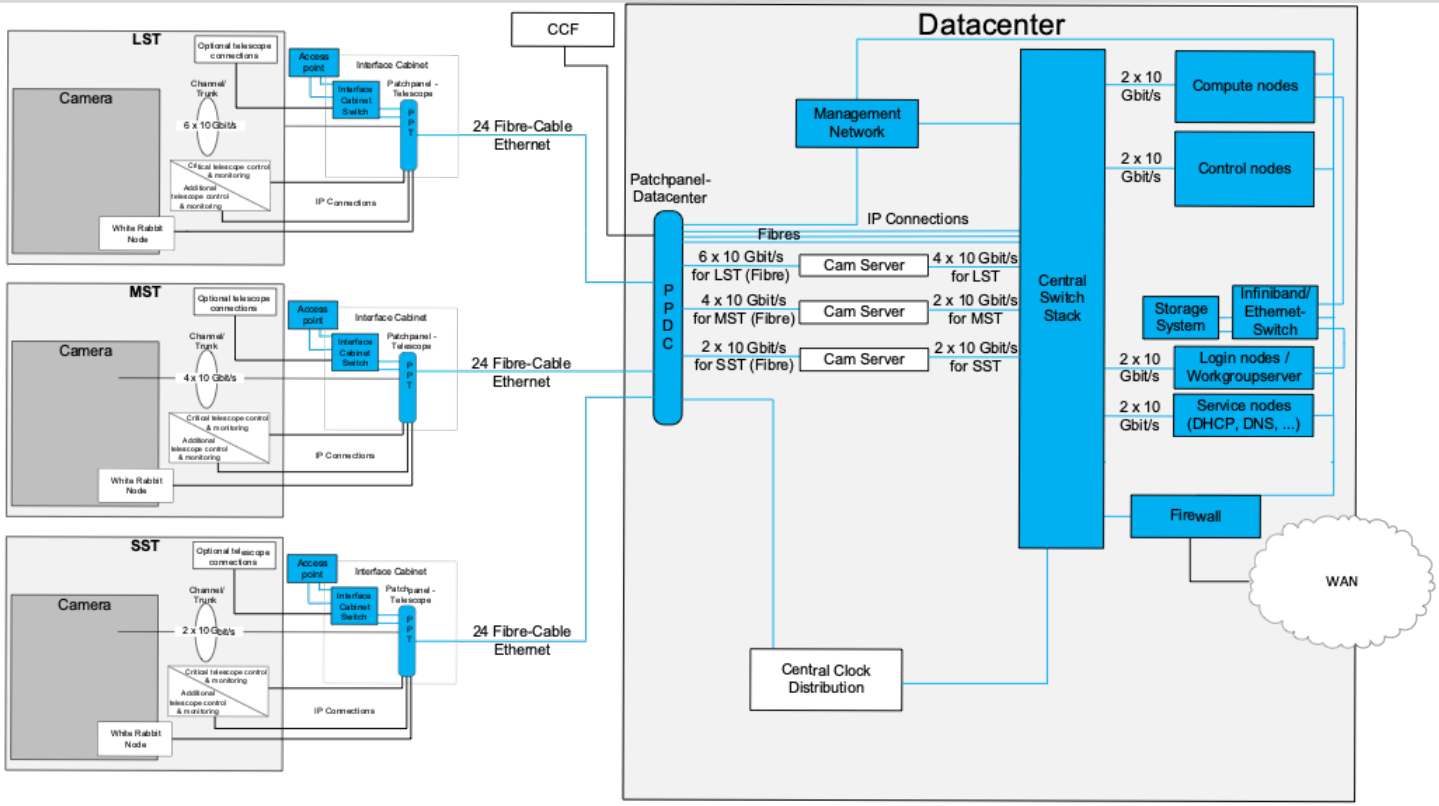
Computer clusters at mainland

Usable for users

Distribute data

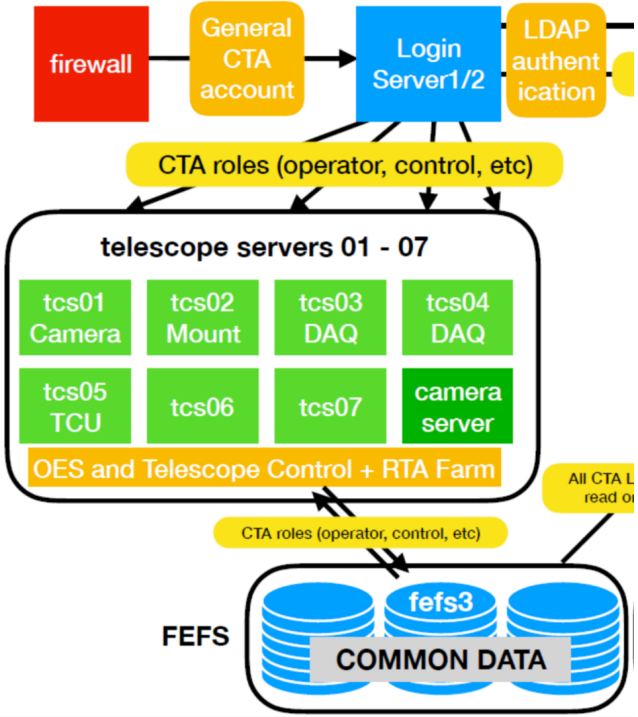
User

Concept & Design for CTA
On-Site ICT Infrastructure - Scope

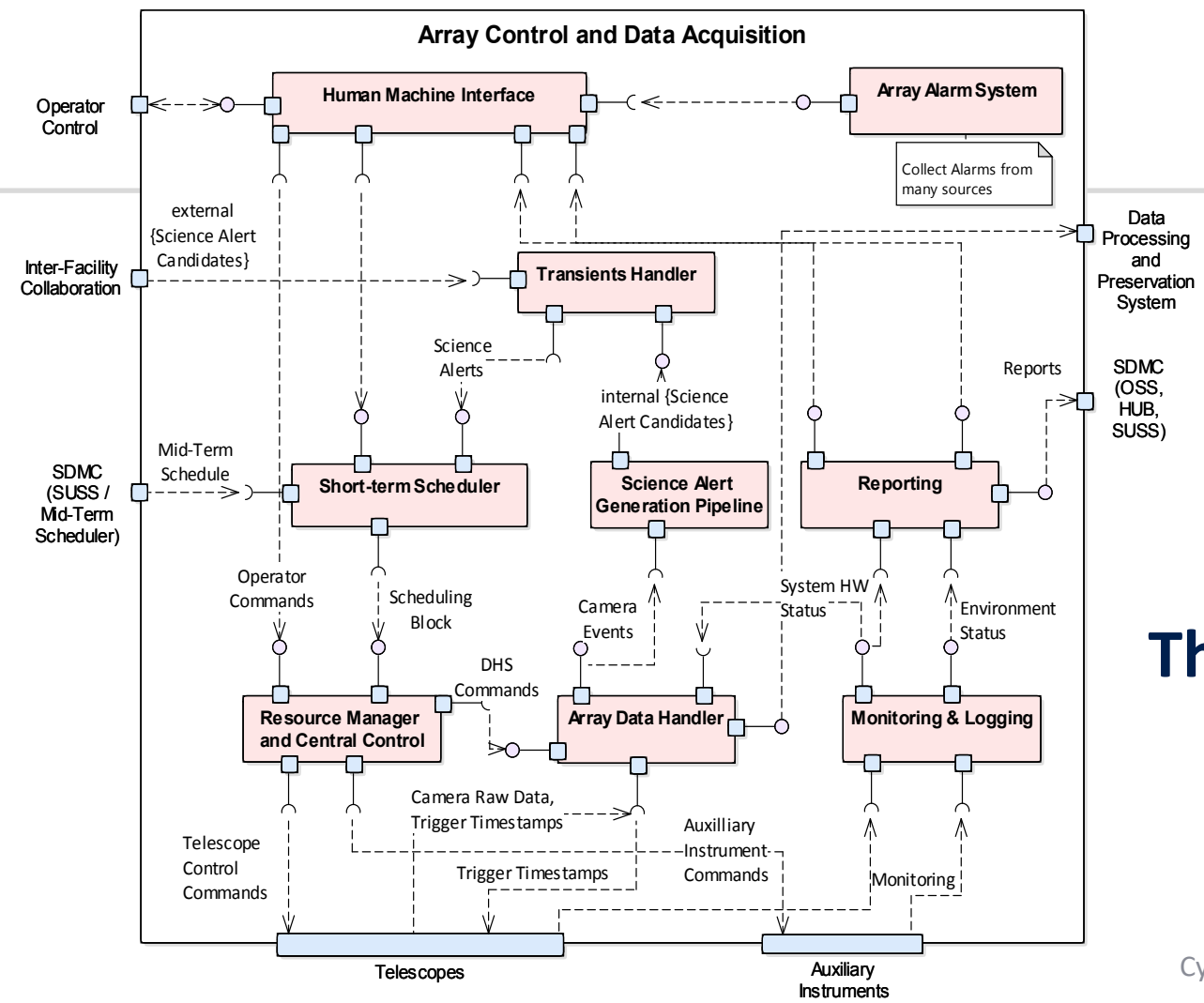


Concept Design for CTA On-Site ICT Infrastructure, 2018

Currently at La Palma – Not yet accepted by CTAO



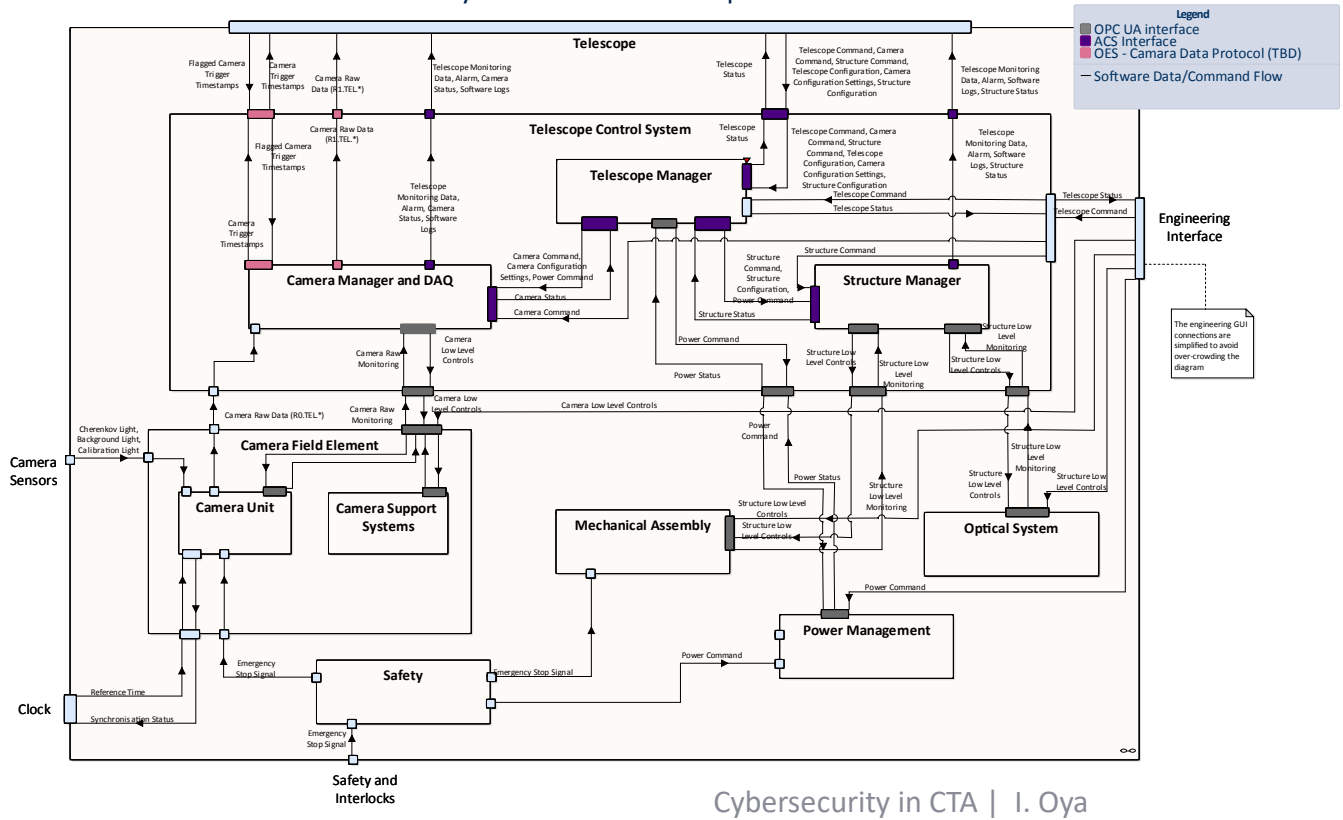
- Currently owned by a Telescope team, planned to be transferred to the CTAO
- It contains:
  - Control system of the 1st telescope
  - Some ACADA prototypes
  - Analysis prototypes



The ACADA System

Telescope decomposition

To Array Control and Data Acquisition



Notes:

- Approximate decomposition, slightly differences in different telescope types
- Some auxiliary systems similar, others more simple